ISTITUTO COMPRENSIVO SAN VITTOR
C.F. 97616430589 C.M. RMIC8CN00V
A09P224 - I.C SAN VITTORINO CORCOLLE
Prot. 0003679/U del 02/05/2023 10:01 I.1 - Normativ

MINISTERO DELL'ISTRUZIONE E DEL MERITO
UFFICIO SCOLASTICO REGIONALE PER IL LAZIO
I.C. SAN VITTORINO - CORCOLLE
Via Spinetoli, 96 - 00132 - ROMA
☎062203507-fax062203507
e-mail rmic8cn00v@istruzione.it pec rmic8cn00v@pec.istruzione.it
codice univoco fatturazione elettronica: UF1ZLY
C.F. 97616430589 C.M. RMIC8CN00V

Roma, 02/05/2023
CIRC 158
Prot vedere segnatura

A tutto il Personale
Alle Famiglie degli alunni

Al Sito WEB

OGGETTO: Regolamenti interni Personale Scolastico e Alunni sull'uso della piattaforma cloud di Istituto (Google Workspace, detta GSuite), aggiornati al 30/04/2023.

Si trasmettono con la presente i due regolamenti in oggetto (aggiornati al 30/04/2023) e si chiede ai Docenti di informarne le Famiglie.
I regolamenti sono visionabili anche sul sito della scuola alla pagina PTOF

Si ringraziano tutti per la consueta collaborazione

Il Dirigente Scolastico
dott.ssa Caterina Biafora
firmato digitalmente ai sensi del CAD
e norme connesse

ISTITUTO COMPRENSIVO SAN VITTOR
C.F. 97616430589 C.M. RMIC8CN00V
A09P224 - I.C SAN VITTORINO CORCOLLE
Prot. 0003652/U del 30/04/2023 14:59 I.4 - Archivio

MINISTERO DELL'ISTRUZIONE E DEL MERITO
UFFICIO SCOLASTICO REGIONALE PER IL LAZIO
I.C. SAN VITTORINO - CORCOLLE
Via Spinetoli, 96 - 00132 - ROMA
☎062203507-fax062203507
e-mail rmic8cn00v@istruzione.it pec rmic8cn00v@pec.istruzione.it
codice univoco fatturazione elettronica: UF1ZLY
C.F. 97616430589 C.M. RMIC8CN00V

Roma, 30/04/2023
Prot. vedere segnatura

REGOLAMENTO INTERNO PER L'UTILIZZO SICURO DI PIATTAFORME CLOUD DI DIDATTICA DIGITALE (aggiornato al 30/04/2023)

Articolo 1: Introduzione

Il presente regolamento è finalizzato a fornire istruzioni al personale della scuola sull'utilizzo sicuro delle piattaforme cloud didattica digitale, come Google Workspace for Education o Office 365 Education. L'utilizzo delle piattaforme cloud è essenziale per garantire un'esperienza di apprendimento online e digitale, ma è altrettanto importante prevenire qualsiasi rischio per la sicurezza dei dati personali degli studenti.

Articolo 2: Registrazione e Accesso

Al momento della registrazione l'amministratore della piattaforma cloud aprirà un profilo con il nome e cognome dell'utente cui verrà associato una casella email istituzionale. Nessun altro dato personale verrà caricato sulla piattaforma e l'utente stesso è invitato a non aggiungere nel proprio profilo altri dati personali quali indirizzo di residenza, numero di telefono, email personale o foto. L'accesso alle applicazioni ed ai servizi della piattaforma avverrà per mezzo dell'indirizzo email istituzionale e la digitazione della relativa password di accesso. È vietato condividere le credenziali di accesso o l'account con altre persone, incluso il personale della scuola o gli studenti.

Articolo 3: Uso di altre applicazioni

Il personale è tenuto ad utilizzare esclusivamente le piattaforme cloud autorizzate dalla scuola, essendo vietato l'utilizzo di piattaforme cloud o di applicazioni non autorizzate o non sicure. Ove i docenti volessero adottare nuove applicazioni dovranno sottoporle all'approvazione del dirigente scolastico che dovrà valutarne il grado di sicurezza.

Articolo 4: Protezione dei Dati Personali

Il personale della scuola è tenuto a rispettare rigorosamente la normativa sulla privacy e sulla protezione dei dati personali degli studenti, in linea con la base legale del trattamento prevista per l'esecuzione del pubblico servizio. Pertanto, è vietato raccogliere, utilizzare o divulgare qualsiasi informazione personale degli studenti senza il rispetto delle norme di legge e senza la supervisione del responsabile della privacy della scuola. Nell'uso della piattaforma ciascun utente deve adottare un principio di minimizzazione dei dati personali in modo che questi non siano presenti se non necessari. Tale principio di minimizzazione deve

essere adottato in modo particolarmente stringente e rigoroso per i dati che rivelano l'origine razziale od etnica, le convinzioni religiose, filosofiche, le opinioni politiche, l'appartenenza sindacale, relativi alla salute o alla vita sessuale (dati sensibili). I docenti dovranno tenere presenti tali principi anche nell'assegnazione delle attività e dei compiti agli alunni che, ove possibile, non dovranno rilevare dati personali ed in particolare sensibili.

Articolo 5: Condivisione di contenuti

Il personale della scuola è responsabile dei contenuti condivisi su piattaforme cloud di supporto alla didattica. Pertanto, si richiede al personale di verificare accuratamente la correttezza e l'accuratezza dei contenuti prima di condividerli e di evitare la condivisione di contenuti offensivi, discriminatori o illegali. Inoltre, è vietato utilizzare le piattaforme cloud per la condivisione di contenuti protetti da copyright o di proprietà intellettuale senza l'autorizzazione esplicita del proprietario.

Articolo 6: Sicurezza

Il personale della scuola deve utilizzare le piattaforme cloud di supporto alla didattica in modo sicuro e responsabile, garantendo la protezione dei dati personali propri e degli studenti che dovranno essere quelli minimi necessari per lo svolgimento delle attività programmate. Pertanto, si richiede al personale di non installare o utilizzare software non autorizzati o non sicuri e di mantenere costantemente aggiornati i propri dispositivi con gli ultimi aggiornamenti di sicurezza. Inoltre, è vietato accedere alle piattaforme cloud da reti pubbliche non sicure.

Articolo 7: Utilizzo corretto delle risorse

Il personale della scuola è tenuto a utilizzare le piattaforme cloud di supporto alla didattica solo per scopi accademici e didattici. L'uso delle piattaforme cloud per attività personali o commerciali non è consentito. Inoltre, è vietato utilizzare le piattaforme cloud per la pubblicità, la propaganda politica o qualsiasi altra attività che possa essere considerata inappropriata o che possa violare le leggi applicabili o le politiche della scuola.

Articolo 8: Archiviazione dei dati

Tutti i dati archiviati nelle piattaforme cloud di supporto alla didattica devono essere adeguatamente protetti da accessi non autorizzati, perdite o danneggiamenti. Il personale deve quindi assicurarsi che i file contenenti dati personali siano salvati in aree sicure delle piattaforme, con accesso limitato solo ai membri del personale o agli studenti o ai genitori autorizzati. Tale accorgimento deve essere adottato in modo particolarmente rigoroso nel caso in cui si debbano archiviare nella piattaforma dati sensibili valutando l'opportunità di adottare anche tecniche di pseudonimizzazione (vedi art. 11).
Inoltre, è importante tenere sotto controllo lo spazio di archiviazione e assicurarsi di cancellare periodicamente i dati non più necessari, al fine di mantenere la sicurezza e la privacy delle informazioni degli studenti. In particolare a fine anno scolastico dovranno essere cancellati, ed eventualmente riconsegnati, tutti i documenti ed elaborati prodotti dagli studenti nel corso dell'anno ad eccezione. Per gli elaborati sottoposti a valutazione si ricorda la Circolare n° 44 del 19/12/2005 della Direzione Generale per gli archivi - "Archivi delle Istituzioni Scolastiche" che prescrive la conservazione per almeno un anno, e la conservazione di documentazione a campione un anno ogni dieci.

Articolo 9: Accesso ai dati

Il personale deve assicurarsi che l'accesso ai dati degli studenti sia limitato solo ai membri del personale autorizzati che necessitano di tali informazioni per svolgere il loro lavoro. In caso di dubbio, il personale deve contattare il Dirigente o il Responsabile della Protezione dei Dati per ottenere conferma del fatto che il trattamento di un particolare set di dati sia giustificato.

Articolo 10: Sicurezza delle password

Il personale deve utilizzare password robuste e complesse per accedere alle piattaforme cloud di sostegno alla didattica. Le password devono essere uniche e non utilizzate in altre piattaforme o servizi. Inoltre, le password devono essere cambiate regolarmente per prevenire accessi non autorizzati.

Articolo 11 – uso di tecniche di pseudonimizzazione per dati ex Art. 9 GDPR

Ai fini della presente sezione, per "dati sensibili" si intendono le categorie di dati personali di cui all'articolo 9 del Regolamento generale sulla protezione dei dati (GDPR) ovverosia dati che rivelano l'origine razziale od etnica, le convinzioni religiose, filosofiche, le opinioni politiche, l'appartenenza sindacale, relativi alla salute o alla vita sessuale. Per queste categorie di Dati Personali, il personale della scuola deve garantire la massima sicurezza e riservatezza in conformità con quanto previsto dal GDPR e dal Codice della privacy. I dati personali di natura sensibile potranno essere caricati sulla piattaforma cloud **solo se strettamente necessari ed in assenza di valide soluzioni alternative**. In questo caso il personale della scuola è tenuto ad utilizzare tecniche di anonimizzazione o pseudonimizzazione (che prevede la sostituzione dei dati personali identificativi dell'interessato -come il nome ed il cognome- con un codice che non consente l'identificazione dell'interessato senza l'utilizzo di ulteriori informazioni). Tali tipi di tecniche devono essere applicati a tutti i dati sensibili, compresi quelli relativi alla salute degli studenti e del personale della scuola, qualora questi siano oggetto di trattamento.

Articolo 12: Sicurezza del dispositivo

Il personale deve utilizzare solo dispositivi sicuri e aggiornati per accedere alle piattaforme cloud di sostegno alla didattica. I dispositivi personali non devono essere utilizzati per accedere a dati sensibili degli studenti, a meno che non siano adeguatamente protetti da password robuste e software di sicurezza aggiornato.

Articolo 13: Gestione delle violazioni dei dati personali

Per la gestione delle violazioni di dati personali (data breach) l'istituto ha definito specifiche linee guida e ha emesso una circolare per il personale in modo che questo sia in grado di riconoscere l'occorrenza di qualunque violazione, anche solo potenziale o sospetta, e di adottare comportamenti conseguenti. Ricordiamo in questa sede le disposizioni che impongono di informare l'amministratore della piattaforma cloud ed il dirigente scolastico di qualunque violazione di dati personali di cui si venga a conoscenza. Per informazioni o richieste di chiarimenti può essere contattato anche il responsabile protezione dati nominato dal dirigente scolastico. Il personale deve cooperare pienamente con qualsiasi indagine interna o esterna relative ai data breach o alle violazioni del presente documento. Le violazioni della presente politica saranno affrontate con la massima serietà e potranno comportare azioni disciplinari fino al licenziamento.

Il Dirigente Scolastico
Dott.ssa Caterina Biafora
Firmato digitalmente ai sensi del CAD
e norme connesse

ISTITUTO COMPRENSIVO SAN VITTOR
C.F. 97616430589 C.M. RMIC8CN00V
A09P224 - I.C SAN VITTORINO CORCOLLE
Prot. 0003653/U del 30/04/2023 15:17 I.4 - Archivio

MINISTERO DELL'ISTRUZIONE E DEL MERITO
UFFICIO SCOLASTICO REGIONALE PER IL LAZIO
I.C. SAN VITTORINO - CORCOLLE
Via Spinetoli, 96 - 00132 - ROMA
☎062203507-fax062203507
e-mail rmic8cn00v@istruzione.it pec rmic8cn00v@pec.istruzione.it
codice univoco fatturazione elettronica: UF1ZLY
C.F. 97616430589 C.M. RMIC8CN00V

Roma, 30/04/2023
Prot. vedere segnatura

Famiglie e Alunni

Norme di comportamento per l'uso della piattaforma cloud nella conduzione delle attività didattiche da parte dello studente

(aggiornato al 30/04/2023)

Nello svolgimento delle attività didattiche e formative avviate dall'istituto lo studente, anche con l'aiuto dei genitori, dovrà garantire il rispetto delle regole di seguito esposte:

Norme generali

- **Rispettare gli altri utenti:** trattare gli altri con rispetto e cortesia, evitare comportamenti offensivi, provocatori o intimidatori
- **Utilizzare un linguaggio appropriato:** utilizzare un linguaggio corretto e rispettoso, evitare l'uso di parole volgari, offensive o discriminatorie.
- **Non disturbare gli altri durante le lezioni:** durante le lezioni a distanza, evitare comportamenti che possano disturbare gli altri alunni, come ad esempio interrompere continuamente il professore o fare rumore di sottofondo.
- **Non utilizzare la piattaforma per scopi non didattici:** utilizzare la piattaforma solo per scopi didattici e comunque autorizzati dal docente, evitando di utilizzarla per fini personali o non correlati al contesto scolastico.
- **Non curiosare sul lavoro di altri utenti:** quando si condividono documenti non si deve interferire, danneggiare o semplicemente curiosare sul lavoro degli altri utenti;
- **Non interagire con estranei:** evitare di interagire con estranei o sconosciuti sulla piattaforma, anche se sembrano essere altri studenti.

Accesso ed uso corretto alla piattaforma

- **L'accesso alla/e piattaforma/e ed ai servizi è strettamente personale:** l'utente accetta di essere riconosciuto quale autore dei messaggi inviati dal suo account e di essere il ricevente dei messaggi spediti al suo account.
- **Sei responsabile del tuo account:** ogni studente è responsabile dell'attività che effettua tramite l'account personale. Non condividere il proprio account con altri studenti o con persone esterne all'istituto
- **Mantenere riservate le tue credenziali:** ogni studente si impegna a conservare in sicurezza e mantenere segreta la password personale di accesso alle piattaforme di didattica a distanza senza consentirne l'uso ad altre persone;
- **Utilizzare le funzionalità della piattaforma correttamente:** utilizzare le funzionalità della piattaforma solo per le finalità a cui sono destinate e rispettando i limiti di utilizzo stabiliti.
- **Non fare spamming:** non inviare messaggi non richiesti o spamming a gli altri utenti.
- **Non rubare l'identità di altre persone:** non rubare l'identità di altre persone, non creare profili falsi o impersonare altre persone.
- **Non copiare o plagiare:** evitare di copiare o plagiare il lavoro degli altri, sia esso un compito, un progetto o altro.
- **Non abusare della connessione internet:** evitare di abusare della connessione internet durante le lezioni, ad esempio evitando di scaricare grandi quantità di dati o di utilizzare applicazioni che potrebbero compromettere la qualità della connessione per gli altri utenti.

Privacy

- **Non divulgare informazioni personali:** non condividere informazioni personali o riservate di se stessi o di altri, come l'indirizzo di casa o il numero di telefono.
- **Non aggiungere informazioni personali nel tuo profilo:** non aggiungere informazioni personali al tuo profilo a quelle già caricate dall'amministratore (come ad esempio indirizzo di residenza, numero di telefono, email personale o foto)
- **Non utilizzare dati personali se non sono necessari:** adotta un principio di minimizzazione dei dati personali in modo che questi non siano presenti sui tuoi elaborati se non necessari.
- **Fai particolare attenzione ai dati sensibili:** il principio di minimizzazione deve essere adottato in modo particolarmente stringente e rigoroso per i dati che rivelano l'origine razziale od etnica, le convinzioni religiose, filosofiche, le opinioni politiche, l'appartenenza sindacale, relativi alla salute o alla vita sessuale (dati sensibili).
- **Non diffondere foto o filmati:** è vietato diffondere in rete o sui social le attività svolte sulla piattaforma anche in forma di foto o di riprese video o vocali;
- **Non diffondere contenuti inappropriati:** non condividere immagini, video, o altri contenuti inappropriati, offensivi o che possano ledere la privacy degli altri.

Proprietà intellettuale

- Rispetta la proprietà intellettuale, non violare i diritti d'autore e non utilizzare il lavoro o i materiali di altri senza autorizzazione

Riprese dal device dello studente durante l'attività da remoto

- La ripresa video dal *device* dello studente deve avere un angolo visuale che permetta l'inquadramento del solo studente, escludendo il più possibile la ripresa degli ambienti familiari o del luogo ove è situata la postazione.

- Lo studente deve trovarsi in un ambiente "neutro" che non presenti segni distintivi o familiari (es. fotografie, poster, oggetti personali, etc.).
- Durante il collegamento video sono da evitare il passaggio o la ripresa di altri componenti del nucleo familiare e comunque di soggetti differenti rispetto allo studente.

Segnalazioni

- Lo studente, anche per il tramite dei genitori deve avvisare l'Istituto nel caso in cui dovesse ricevere materiale audio, video, PPT, etc. non pertinente al percorso didattico avviato o lesivo dei diritti di qualcuno; in tale ipotesi le segnalazioni dovranno essere inviate al seguente indirizzo email: rmic8cn00v@istruzione.it
- E' obbligatorio segnalare immediatamente l'impossibilità ad accedere al proprio account, l'eventuale smarrimento o furto delle credenziali personali o qualunque situazione che possa determinare un furto di identità.

Misure di sicurezza informatica

- Effettua costantemente gli aggiornamenti di sicurezza del sistema operativo del device che utilizzi per accedere alla piattaforma o ai servizi di didattica a distanza
- Assicurati che i software di protezione del tuo sistema operativo (Firewall, Antivirus, ecc) siano abilitati e costantemente aggiornati
- Assicurati che il device che utilizzi per accedere alla DAD sia protetto da una password di almeno 8 caratteri contenente una lettera maiuscola, un numero ed un carattere speciale
- Blocca l'accesso al sistema e/o configura la modalità di blocco automatico quando ti allontani dalla postazione di lavoro
- Non cliccare su link o allegati contenuti in email sospette
- Utilizza l'accesso a connessioni Wi-Fi adeguatamente protette

La violazione delle norme del presente regolamento può comportare provvedimenti disciplinari da parte della scuola che non precludono ulteriori interventi delle autorità competenti nel caso in cui tali comportamenti comportassero la violazione della normativa in materia di tutela del diritto d'autore (L. 633/1941 e ss. mm. e ii.) nonchè della normativa in tema di tutala dei dati personali (D. Lgs 196/2003 e ss. mm. e ii. e Regolamento UE 679/2016 – GDPR). La scuola ha adottato tutte le misure preventive atte ad evitare che gli strumenti adottati per la DAD possano essere utilizzati per atti di cyberbullismo che verranno sempre puniti con la massima severità ove rilevati.

Ricordando la responsabilità dei genitori e dei tutori previste all'art. 2048, si chiede la loro fattiva collaborazione, ove possibile e necessario, per superare eventuali difficoltà all'uso degli strumenti informatici da parte degli alunni e, sempre, per vigilare sul rispetto del presente regolamento.

Il Dirigente Scolastico
Dott.ssa Caterina Biafora
Firmato digitalmente ai sensi del CAD
e norme connesse